

# ОСОБЕННОСТИ ПОИСКОВОЙ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## FEATURES SEARCH ACTIVITY THE INVESTIGATOR IN SOLVING CRIMES IN THE SPHERE OF COMPUTER INFORMATION

**A. Belousov  
Z. Vassalatiy**

*Summary.* The article is devoted features search activity the investigator in solving crimes in the sphere of computer information. An attempt is made to determine the criminalistic essence and highlight the informational significance of the process of crime detection, as well as, depending on the current investigative situation, to develop an algorithm for the investigator's search activity in the disclosure of crimes in the field of computer information.

*Keywords:* crime; computer information; investigative situation; verification of a crime report; preliminary investigation.

**Белоусов Алексей Владимирович**

*К.ю.н., доцент, Тюменский Государственный  
Университет  
belousovalecs@mail.ru*

**Вассалатий Жанна Васильевна**

*К.ю.н., доцент, Тюменский Государственный  
Университет  
z.v.vassalatiy@utmn.ru*

*Аннотация.* Статья посвящена особенностям поисковой деятельности следователя при раскрытии преступлений в сфере компьютерной информации. Предпринята попытка определить криминалистическую сущность и выделить информационную значимость процесса раскрытия преступлений, а также в зависимости от сложившейся следственной ситуации разработать алгоритм поисковой деятельности следователя при раскрытии преступлений в сфере компьютерной информации.

*Ключевые слова:* преступление; компьютерная информация; следственная ситуация; проверка сообщения о преступлении; предварительное расследование.

**Н**а сегодняшний день преступления рассматриваемого вида в большинстве случаев остаются нераскрытыми, а также характеризуются как латентные.

Анализ практической деятельности правоохранительных органов при расследовании рассматриваемого вида преступлений, теоретических положений и действующего законодательства, позволил акцентировать внимание на особенности поисковой деятельности следователя в получении информации о совершении преступления определенным лицом.

Поисковая деятельность следователя преимущественно проявляется в процессе раскрытия преступления. Представленные в теории криминалистики точки зрения ученых [1–4] указывают на то, что процесс раскрытия присутствует в ходе досудебного и судебного производства по уголовному делу. Позволяя таким образом проверить и подтвердить выдвинутые версии.

Кроме вышеизложенного, для всех правоохранительных органов, на законодательном уровне подчеркивается, что к нераскрытым преступлениям относятся

уголовные дела, производство по которым приостановлено (п.п. 1–3 ч. 1 ст. 208 УПК РФ). Исключением являются, преступления по которым вступило в законную силу обвинительное или оправдательное судебное решение, постановление о прекращении уголовного дела, судебное решение о применении принудительных мер медицинского характера [5].

В результате указанного выше проведенного анализа под процессом раскрытия преступления считается совместная деятельность следователя, оперативных подразделений и суда направленная на получение информации, представляющая основание для выдвижения, проверки, подтверждения процессуальными действиями версии о совершении преступного события конкретным лицом после того, как все иные взаимоисключающие ее версии будут проверены и отвергнуты.

Анализ статистических данных по преступлениям в сфере компьютерной информации показывает, зарегистрировано преступлений: 2019 г.— 2883, 2020 г.— 4498, 2021 г.— 6869. Раскрыто: 2019 г.— 729, 2020 г.— 830, 2021 г.— 1545. Выявлено лиц: 2019 г.— 319, 2020 г.— 389, 2021 г.— 462. Направлено в суд: 2019 г.— 468, 2020 г.— 480, 2021 г.— 1155. [6–8]

Представленные данные свидетельствуют не только о росте совершаемых преступлений, но и низкой раскрываемости.

Таким образом организация поисковой деятельности следователя требует постоянной трансформации в ходе досудебного производства по уголовным делам рассматриваемого вида преступлений.

Проведенный теоретический [См., например: 9–13] и эмпирический анализ показывает, что по рассматриваемым преступным деяниям наибольшую сложность для следственных подразделений представляют типичные следственные ситуации с неустановленным лицом, а именно: указанным лицом совершен неправомерный доступ и воздействие на компьютерную информацию; нарушены правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; использована и распространена вредоносная компьютерная программа.

Выдвигаемыми версиями в представленных следственных ситуациях, являются: к преступлению причастны близкие родственники, друзья знакомые имеющие удаленный или прямой доступ к компьютерно-телекоммуникационному техническому средству физического лица; к преступлению причастно лицо из состава администрации или персонала юридического лица, а также ранее работавшие и уволенные по отрицательным мотивам; к преступлению причастны посторонние лица, находившиеся на территории юридического лица в период совершения преступления; к преступлению причастно лицо, ранее судимое за аналогичные преступления; к преступлению причастны недобросовестные конкуренты юридического лица; к преступлению причастны запрещенные в России организации; цель скрыть уже ранее совершённое преступление; неправомерный доступ, воздействия на компьютерную информацию или распространение вредоносных компьютерных программ произошел в результате электронного документооборота между юридическим лицом и участниками предпринимательской деятельности; произошел непреднамеренный технический сбой в работе компьютерно-телекоммуникационного технического средства; заявитель в силу своих слабых пользовательских познаний с компьютерно-телекоммуникационным техническим средством заблуждался и ошибочно обратился с заявлением о совершенном преступлении в правоохранительные органы.

Таким образом задачами будут являться:

- ◆ сведения, доказывающие неправомерный доступ и воздействие на компьютерную информацию;

- ◆ нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- ◆ создание, использование и распространение вредоносных компьютерных программ;
- ◆ поиск лица, совершившего преступление.

В результате чего можно предложить следующую программу (алгоритм) поисковых действий следователя:

#### На этапе возбуждения уголовного дела

*Опрос* необходим для определения обстоятельств (времени, места, условий) и способа совершения преступления, а в отдельных случаях описать внешность заподозренного лица в противоправных действиях. *Осмотр места происшествия* необходим для определения места совершения преступления, обнаружения, фиксации и изъятия следов (например: неправомерного доступа и воздействия на компьютерную информацию; нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; создания, использования и распространения вредоносных компьютерных программ (червь, троян, spyware, adware, keylogger, ботнет, руткит, баннеры вымогатели, фишинг, спам), а так же следы пальцев, ладоней руки и обуви). *Исследования* изъятых компьютерно-телекоммуникационных технических средств, их компонентов или системного обеспечения в лабораторных условиях, на предмет обнаружения следов преступления. *Истребование у юридического лица документов*, например, должностные инструкции, документы финансовой отчетности, локальные акты, регулирующие эксплуатацию, хранение, обработку или передачу компьютерной информации и информационно-телекоммуникационных сетей. *Истребование видеофайлов охранной системы видеонаблюдения* необходимо для установления виновного в совершении противоправных деяния, способа совершения, идентификации объектов имеющих отношение к произошедшему преступному деянию. *Проведение ревизии* необходимо для выявления действий по использованию вредоносных компьютерных программ для снижения или неуплаты налогов. *Использование информационно-справочных учетов*: правоохранительных органов: оперативно-розыскные, розыскные, криминалистические, по линии Национального центрального бюро Интерпол; провайдеров предоставления услуги доступа к сети интернет и иным связям. *Письменное поручение о проведении оперативно-розыскных мероприятий*, необходимо для получения сведений

и объектов: о лице, совершившем неправомерный доступ и воздействие на компьютерную информацию, его подельниках; его местонахождении; месте откуда осуществлялся или осуществляется неправомерный доступ и воздействие на компьютерную информацию; месте сокрытия объектов, содержащих вредоносную компьютерную программу; месте хранения цифровых носителей информации; сведения о перечне электронных документов финансовой отчетности подвергшихся неправомерному доступу и воздействию вредоносной компьютерной программой; места хранения записных книжек или черновики содержащих пароли, электронные ключи для преодоления средств защиты от неправомерного доступа к компьютерной информации; сведения о способе и какие средства использовались для неправомерного доступа и воздействия на компьютерную информацию.

#### На этапе предварительного расследования

*Допрос потерпевшего, свидетелей, эксперта, специалиста* позволит, используя тактические приемы и их комбинацию уточнить, детализировать, сопоставить интересующую следствие сведения об обстоятельствах произошедшего преступного события и лицах, совершивших данное преступное деяние. Допрос *подозреваемого (обвиняемого)* позволит установить каковы цели и мотивы совершения преступления, навыки и уровень пользования с электронно-телекоммуникационным устройством, место работы, имеет ли доступ к указанному устройству на работе, что входит в его обязанности на рабочем месте (если преступление связано с местом работы) [13, с. 96]. *Очная ставка* позволяет устранить противоречия, проверить правдивость показаний, используя тактические приемы уличить во лжи. *Проверка показаний на месте* необходима для выяснения противоправных действий и обнаружения новых доказательств. *Обыск и выемка* необходима для обнаружения рукописных записей в виде цифр, букв, знаков, которые могут обозначать пароли или машинный код (например, машинный код вредоносной программы), должностные инструкции; локальные нормативные акты регулирующие правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей организации,

документы финансовой отчетности. *Осмотр и приобщение вещественных доказательств к уголовному делу* позволяет сделать вывод об относимости, допустимости, достоверности осматриваемого объекта к уголовному делу, а также выделить общие и частные признаки. *Судебная компьютерно-техническая экспертиза* позволяет установить: модель компьютерно-телекоммуникационного технического средства; технические характеристики электронного компонента компьютерно-телекоммуникационного технического средства; где, когда изготовлено или собрано данное компьютерно-телекоммуникационное техническое средство, каковы его комплектующие; были ли внесены программные изменения; исправность самого компьютерно-телекоммуникационного технического средства и его электронных компонентов; причины неисправности; установить операционную систему; содержание информации в памяти компьютерно-телекоммуникационного технического средства; стандартность и лицензионность электронной программы; изменения электронной программы; признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; реализована ли в компьютерной системе какая-либо система защиты доступа к информации; имеются ли программы с признаками вредоносности; каково содержание установок удаленного доступа и протоколов соединений; имеют ли комплектующие компьютерно-телекоммуникационного технического средства единое происхождение [14, с. 109–111]. *Отдельные поручения о производстве следственных действий, оперативно-розыскных мероприятий, международные поручения* позволяют организовать взаимодействие с целью обмена информацией относящейся к преступному событию, устранить разобщенность между участниками расследования, оперативно провести совместные следственные действия и оперативно-розыскные мероприятия. *Взаимодействие со средствами массовой информации* позволит дезинформировать и предотвратить попытки противодействия со стороны лиц причастных к совершению преступного деяния.

Таким образом, представленный алгоритм (программа) поисковых действий следователя позволяет повысить эффективность раскрытия преступлений в сфере компьютерной информации.

#### ЛИТЕРАТУРА

1. Танасевич В.Г. Криминалистическое понятие раскрытия преступления // Социалистическая законность. 1975. № 10. С. 57–58.
2. Белкин Р.С. Курс криминалистики: в 3 т. Т. 3: Криминалистические средства, приемы и рекомендации. М.: Юристъ, 1997. Т. 3. 480 с.
3. Мазунин Я.М. О понятии раскрытия преступления. Совершенствование следственной и экспертной практики: материалы междунар. науч.-практ. конф., Омск, 2 июня 2010 г. Омск: Омская акад. МВД России, 2010. С. 79–83.

4. Суденко В.Е. Раскрытие преступления: оперативно-розыскная и криминалистическая теории. Уголовное производство: процессуальная теория и криминалистическая практика. Материалы VII междунар. науч.-практ. конф. Алушта, 25–26 апреля 2019 г.: ООО «Издательство Типография «Ариал» (Симферополь). 2019. С. 114–116.
5. О едином учете преступлений: приказ Генеральной прокуратуры РФ № 39, МВД РФ № 1070, МЧС РФ № 1021, Минюста РФ № 253, ФСБ РФ № 780, Минэкономразвития РФ № 353, ФСКН РФ № 399 от 29.12.2005 / Зарегистрировано в Минюсте РФ 30.12.2005 № 7339 // Рос газ. 25.01.2006. № 13.
6. Состояние преступности в России за январь-декабрь 2019 год. М.: Главный информационно-аналитический центр МВД России. URL: <https://xn—b1aew.xn—p1ai/reports/item/19412450> (дата обращения: 10.02.2022).
7. Состояние преступности в России за январь-декабрь 2020 год. М.: Главный информационно-аналитический центр МВД России. URL: <https://xn—b1aew.xn—p1ai/reports/item/19412450> (дата обращения: 10.02.2022).
8. Состояние преступности в России за январь-декабрь 2021 год. М.: Главный информационно-аналитический центр МВД России. URL: <https://xn—b1aew.xn—p1ai/reports/item/19412450> (дата обращения: 10.02.2022).
9. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / (А.Ф. Абдулвалиев, А.В. Белоусов, Ж.В. Вассалатий и др.; под науч. ред. проф. Е.В. Смахтина, проф. Р.Д. Шарапова, доц. В.И. Морозова); Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт государства и права. Тюмень: Изд. Тюменского государственного университета, 2021. 376 с.
10. Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: диссертация ... кандидата юридических наук: 12.00.12. Москва, 2015.
11. Гаврилин Ю.В., Аносов А.В., Баранов В.В., Васильченко Д.А. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. Изд-во: Академия управления МВД России. М. 2019. Ч 1. 208 с.
12. Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: автореферат дис. ... кандидата юридических наук: 12.00.12. Ростов-на-Дону, 2020.
13. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: диссертация ... кандидата юридических наук: 12.00.12. Москва, 2016.
14. Кузнецов А.А. Понятие, виды и назначение судебных экспертиз в Российской Федерации: учеб.-справ. Пособие /под общ. ред. проф. А.А. Кузнецова. Изд-во: Омская академия МВД России. Омск, 2014. 164 с.

© Белоусов Алексей Владимирович ( [belousovalecs@mail.ru](mailto:belousovalecs@mail.ru) ), Вассалатий Жанна Васильевна ( [z.v.vassalatij@utmn.ru](mailto:z.v.vassalatij@utmn.ru) ).

Журнал «Современная наука: актуальные проблемы теории и практики»